IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Inventors: Lookman Yasin Fazal et al.

Serial No.: 10/757676

Conf. No.: 8048

Filing Date: 1/14/2004

Art Unit: 2154

Examiner: Michael E. Keefer

Docket No.: 630-053US

Title: Detection of Hidden Wireless Routers

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Enclosed are the following papers related to the above-identified patent application:

- Transmittal Letter
- Appeal Brief

Pursuant to 37 CFR 1.136(a)(3), please treat this and any concurrent or future reply in this application that requires a petition for an extension of time for its timely submission as incorporating a petition for extension of time for the appropriate length of time.

Respectfully,
Lookman Yasin Fazal et al.

By **/Kiril Dimov/**
Kiril Dimov
Reg. No. 60, 490
Attorney for Applicants
732-578-0103 x 215

DeMont & Breyer, L.L.C.
Suite 250
100 Commons Way
Holmdel, NJ 07733
United States of America

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Inventors: Lookman Yasin Fazal et al.

Serial No.: 10/757676

Conf. No.: 8048

Filing Date: 1/14/2004

Art Unit: 2154

Examiner: Michael E. Keefer

Docket No.: 630-053US

Title: Detection of Hidden Wireless Routers

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

APPEAL BRIEF UNDER 37 CFR 41.67

Pursuant to 37 CFR 41.67, this brief is filed in support of the appeal in this application.

TABLE OF CONTENTS

REAL PARTY IN INTEREST

The real party of interest in this application is the assignee of this application: Avaya Technology LLC of Basking Ridge, NJ.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

STATUS OF CLAIMS

Claims 14-17 stand rejected and are being appealed.

STATUS OF AMENDMENTS

All amendments have been entered.

SUMMARY OF THE CLAIMED SUBJECT MATTER

A secure network, such as the network of a major corporation, can be accessed through a secure access server. A secure access server is what the name suggests; It is a server that implements proper security measures and policies to prevent unauthorized access to the corporate network.

However, when a laptop, having both a wired and wireless network adapters, is connected to two networks — one secure and one insecure, the laptop may pose a security threat to the secure network. In particular, the laptop may be configured to receive packets at the network adapter connected to the insecure network and forward the packets to the secure network via the other network adapter which is authorized to access the secure network. When this happens, the laptop is said to act as a hidden router, and it represents a security threat to the secure network.

In other words, a hidden router is a device that connects an insecure network to a secure network without the permission of the system administrator in charge of the secure network. The existence of hidden routers presents a security threat the secure network, and it is, therefore, desirable that a method exists for detecting hidden routers.

The present invention provides one such method. In accordance with the present invention a test station is deployed in a first network, and a test server is deployed in a second "secure" network. The test station generates a protocol data unit in which the destination address is set to the address of the test server. After that, the test station forwards the protocol data unit to a second station that is different from the test server. If the protocol data unit makes its way from the first network, into the second "secure" network, and is received by the test server, then an alarm is raised that a hidden router is detected. (**Specification at paragraph [0013])**

With regard to the function of the second station, it is important to note that the second station, to which the protocol data unit is forwarded, does not necessarily have to be the hidden router. Instead, the second station may forward the packet to a third station; the third station may forward the packet to a fourth station and so forth until the protocol data unit finds its way into the secure network and is received by the test server. (**Specification at paragraph [0032])**

The present invention comprises one (1) independent claim. The claim shall be presented, summarized, and mapped to the specification and the drawings, if any.

Independent claim 14 recites:

> **14.** A method comprising:
>
> deploying a first station in a first network;
>
> deploying a server in a second network connected to said first network through a secure access server;
>
> transmitting from said first station a protocol data unit addressed to a second station in said first network, ***wherein said protocol data unit comprises an address of said server***; and
>
> triggering an alarm if said protocol data unit is received at said server.
>
> (*emphasis supplied*)

Claim 14 is described in the Specification at Paragraphs [0080] – [0085].

GROUNDS OF OBJECTION AND REJECTION TO BE REVIEWED ON APPEAL

Ground 1: 35 U.S.C. 103 Rejection of Claims 14-17

Claims 14 - 14 were rejected under 35 U.S.C. 103(a) as being unpatentable H. Etoh, U.S. Patent 7,159,033 (hereinafter "Etoh") in view of T. Ando, U.S. Patent 6,895,432 (hereinafter "Ando").

ARGUMENTS

Ground 1: Rejection of Claim 15

Claims 14 - 17 were rejected under 35 U.S.C. 103(a) as being unpatentable H. Etoh, U.S. Patent 7,159,033 (hereinafter "Etoh") in view of T. Ando, U.S. Patent 6,895,432 (hereinafter "Etoh"). The applicants respectfully traverse.

Claim 14 recites:

> **14.** A method comprising:
>
> deploying a first station in a first network;
>
> deploying a server in a second network connected to said first network through a secure access server;
>
> transmitting from said first station a protocol data unit addressed to a second station in said first network, ***wherein said protocol data unit comprises an address of said server***; and
>
> triggering an alarm if said protocol data unit is received at said server.
>
> (*emphasis supplied*)

Nowhere does Etho teach or suggest, alone or in combination with the other references, what is recited in claim 14 — namely, the transmission of ordinary protocol data units. The packet generation means, (to use the terminology of Etoh), used in the present invention and Etoh, operate differently.

The invention defined in claim 14 is simpler and more robust that what Etoh teaches, because the present invention does not resort to the use of inspection packets.

The inspection packets in Etoh, are IP packets in which the source address is not the address of the sender, but rather is the address of the reception router search apparatus. Paragraph [0089] of Etoh discusses in detail the structure of the inspection packets:

> … For all the inspection target network connection apparatuses on the list prepared by the list preparation means 41, the IP packet generation means 43 generates an IP packet that designates the IP addressees of these network connection apparatuses as destination IP addresses. **It should be noted that the source IP address of the IP packet generated by the IP packet generation means 43 is not actually the IP address of the transmitter router search apparatus 26, but is instead the IP address of the reception router search apparatus 28.** Finally, IP packet transmission means 44 sequentially outputs, to the intranet 10, IP packets generated by the IP packet generation means 43.
>
> **(Etoh at paragraph 89)**

The invention of claim 14 does not create response packets, as Etoh does, and paragraphs [0081] and [0082] of the present Specification support this contention:

> [0081] At task 1002, a server, test server 209, is deployed in a second network, an example being wireline network portion 220. The first network is connected to the second network through a secure access server, such as secure access server 203.
>
> [0082] At task 1003, test station 208 attempts to send a protocol data unit to test server 209 in the second network via a second station, wireless client 201-3, in the first network. In the illustrative embodiment of the present invention, test station 208 sends the protocol data unit to test server 209 by transmitting to wireless client 201-3 a protocol data unit having a destination address equal to an address of test server 209. In some embodiments, the protocol data unit comprises a network layer address source address of the second station.
>
> **(Specification at pargarphs [0089] and [0090])**

The defined in claim 14 relies on the generation of protocol data units in which **only** the source field needs to be set to the address of a test server.

Furthermore, the invention of claim 14 differs from Etoh on the grounds that the present invention does not serve to identify particular hidden routers; rather the present invention merely detects the existence of a hidden router without necessarily revealing the identity of the hidden router.

The invention of Etoh tests a "list of the IP addresses of all the inspection target network connection apparatuses on the intranet" **(*See* Etoh at paragraph [0089], col. 8, ll. 31-33)** to see if one or more of them are operating as routers. The method described in Etoh is for testing whether a particular device operates as a hidden router, whereas the method of the present invention is for detecting whether a protocol data unit travels from one network into another without necessarily establishing that a particular device on the network acts as a hidden router.

In Etoh, a receipt of a response packet by the recipient router means that the tested inspection target network connection apparatus must be a hidden router:

> **... If the inspection target network connection apparatus is a router, the response IP packet is transmitted by that router across the Internet 19 to the recipient router search apparatus 28. Whereas if the inspection target network connection apparatus is not a router, the response IP packet is transmitted to the intranet 10 where the authorized router 13 inhibits the transmission of the response IP packet from the intranet 10 to the Internet 19, terminating the response IP packet at the intranet 10.** Therefore, when the reception router search apparatus 28 receives a response IP packet, it can be assumed that the inspection target network connection apparatus is a currently operating router.
>
> **(Etoh at paragraph 90, col. 9, ll. 4-13)**

The invention of Etoh inspects a target network connection apparatus to determine if the apparatus is acting as a hidden router.

In contrast, the invention of claim 14 simply detects whether one protocol data unit from a first network can travel into a second network. Paragraph [0085] of the present Specification provides support for this contention:

> [0085] In the event that test server 209 detects an illegitimately routed protocol data unit, in **some embodiments test server 209 can be arranged to record the network layer source address of the protocol data unit, and then use that network layer source address as a means of identifying the logical network location and physical location of the hidden wireless router** so that it can be disabled. For example, in some embodiments of the present invention, the network layer source address as recorded at test server 209 can be used as an index into a database relating network layer addresses of wireline network stations to corresponding wireline network port numbers, thereby obtaining the wireline network port number of the hidden wireless router. Steps can then be taken to disable the network jack associated with that port number, or, alternatively, administrative personnel can physically unplug or otherwise disable the hidden wireless router.
>
> **(Specification at paragraph [0085])**

In accordance with the present invention, a receipt of the protocol data unit by the test server, does not automatically mean that the second station or any other particular device on the network is a hidden router, rather additional tasks to those defined in claim 14 need be executed in order to determine the identity of the hidden router.

In light of the foregoing arguments, and because Ando fails to cure the deficiencies of Etoh, the applicants respectfully submit that the rejection of claim 14 is traversed.

Because claims 15-17 depend on claim 14, the applicants respectfully submit that the rejection of them is also traversed.

CONCLUSION

The applicants have demonstrated that the logic underlying the Office's rejection is untenable, and, therefore, that the rejection is not sustainable. For this reason, the applicants respectfully request the Board of Appeals to reverse the decision of the Examiner as provided for in 37 C.F.R. 41.50(a).

Respectfully,
Lookman Yasin Fazal et al.

By **/Kiril Dimov/**
Kiril Dimov
Reg. No. 60, 490
Attorney for Applicants
732-578-0103 x 215

DeMont & Breyer, L.L.C.
Suite 250
100 Commons Way
Holmdel, NJ 07733
United States of America

Claims Appendix

1. (Withdrawn) A method comprising:

receiving a protocol data unit that comprises a destination address; and

transmitting an alarm when said destination address is not associated with a secure access server.

2. (Withdrawn) The method of claim 1 wherein said destination address is a data link layer address.

3. (Withdrawn) The method of claim 1 wherein said destination address is a network layer address.

4. (Withdrawn) The method of claim 1 wherein said destination address is associated with a device that is associated with: (i) a network layer address in a first network, and (ii) a network layer address in a second network, wherein said first network and said second network are different.

5. (Withdrawn) The method of claim 4 wherein said alarm comprises at least one of (i) said network layer address in a first network, and (ii) said network layer address in a second network.

6. (Withdrawn) A method comprising:

(a) receiving a protocol data unit that comprises a data link layer destination address and a network layer destination address; and

(b) transmitting an alarm when:

(i) said data link layer destination address is not associated with a secure access server, and

(ii) said network layer destination address is not associated with said secure access server.

7. (Withdrawn) The method of claim 6 wherein said data link layer destination address is associated with a device that is associated with: (i) a network layer address in a first network, and (ii) a network layer address in a second network; and

wherein said alarm comprises at least one of (i) said network layer address in a first network, and (ii) said network layer address in a second network.

8. (Withdrawn) A method comprising:

receiving in a first network a protocol data unit that comprises a network layer destination address; and

transmitting an alarm when said network layer destination address is a network layer address in a second network.

9. (Withdrawn) The method of claim 8 wherein said protocol data unit further comprises a data link layer destination address;

wherein said data link layer destination address is associated with a device that is associated with: (i) a network layer address in a first network, and (ii) a network layer address in a second network; and

wherein said alarm comprises at least one of (i) said network layer address in a first network, and (ii) said network layer address in a second network.

10. (Withdrawn) A method comprising:

receiving a first protocol data unit that comprises a data link layer destination address and a first network layer destination address;

receiving a second protocol data unit that comprises said data link layer destination address and a second network layer destination address; and

triggering an alarm when said data link layer address is different than the data link layer addresses of all authorized routers and said first network layer destination address is different than said second network layer destination address.

11. (Withdrawn) The method of claim 10 wherein said data link layer destination address is associated with a device that is associated with: (i) a network layer address in a first network, and (ii) a network layer address in a second network; and

wherein said alarm comprises at least one of (i) said network layer address in a first network, and (ii) said network layer address in a second network.

12. (Withdrawn) A method comprising:

receiving a protocol data unit that comprises a data link layer destination address and a network layer destination address; and

triggering an alarm when said data link layer destination address is associated with a different device than is said network layer destination address.

13. (Withdrawn) The method of claim 12 wherein said data link layer destination address is associated with a device that is associated with: (i) a network layer address in a first network, and (ii) a network layer address in a second network; and

wherein said alarm comprises at least one of (i) said network layer address in a first network, and (ii) said network layer address in a second network.

---

14. (Original) A method comprising:

deploying a first station in a first network;

deploying a server in a second network connected to said first network through a secure access server;

transmitting from said first station a protocol data unit addressed to a second station in said first network, wherein said protocol data unit comprises an address of said server; and

triggering an alarm if said protocol data unit is received at said server.

15. (Original) The method of claim 14 wherein said protocol data unit further comprises a network layer source address of said second station; and

wherein said alarm comprises said network layer source address.

16. (Original) The method of claim 15 further comprising obtaining the wireline network port number corresponding to said network layer source address.

17. (Original) The method of claim 16 further comprising disabling the network jack associated with said wireline network port number.

Evidence Appendix

There is no evidence submitted pursuant to 37 CFR §§ 1.130, 1.131, or1.132.

Related Proceedings Appendix

There are no related proceedings.